High Security of Data in Cloud Computing

Deepak Kumar

***Abstract*— Now a days, large scale distributed systems such as cloud computing applications are becoming increasingly popular. But the challenges with these applications like transferring, storing and computation of data have to be dealt with. The most prevalent distributed file systems to deal with these challenges are the Hadoop File System (HDFS) which is a variant of the Google File System (GFS). However HDFS has two potential problems. The first one is that it depends on a single name node to manage almost all operations of every data block in the file system. As a result it can be a bottleneck resource and a single point of failure. The second potential problem with HDFS is that it depends on TCP to transfer data. As has been cited in many studies TCP takes many rounds before it can send at the full capacity of the links in the cloud. This results in low link utilization and longer download times. Our work develops a mechanism of Triple security which uses a light weight front end server to connect all requests with many name nodes. Our work proposes a new distributed file system which will overcome these problems of HDFS.**

***Index Terms*— Cloud Computing, Cryptography, DSA, AES, DES, Steganography**

I. INTRODUCTION

The danger could be the possible fraud by some merchants, also hacking into the electronic records or interception of a transmission is another risk. There is also the danger of human error or equipment failure which can jeopardize the accuracy of transmissions or records. Customers should check their banking records carefully for unfamiliar or unauthorized transactions.

Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. In this research, we clarify what Steganography is, the definition, the importance as well as the technique used in implementing steganography [1]. We focus on the Least Significant Bit (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message. Some of the common taxonomy of Steganographic Techniques are given in Figure 1.

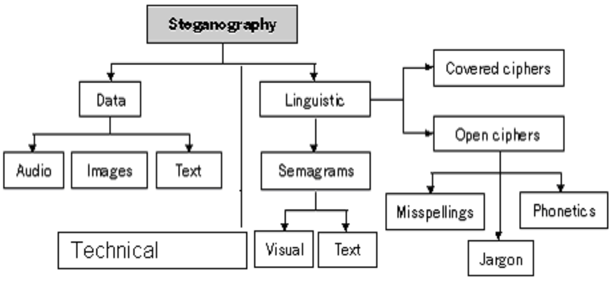


Figure 1: Common Taxonomy of Steganographic techniques

The main features of the proposed work are:

- It eliminates the need of issuing cheque-book from the bank.
- It eliminates cheque portability issue.
- It provides a more secure means of transaction.
- It provides a very fast and reliable means of transaction.
- It lowers the transaction processing time or the clearing cycle.
- It eliminates the need of internet banking infrastructure (for fund transfer) by the banks.
- It maintains the confidentiality and integrity of the transaction details.
- It provides an improved customer service.
- This kind of e-Cheques management is not being developed and used in any of the Banks so far.

To develop a user friendly Electronic Check System to overcome the limitation of manual check system & to enhance the flexibility of the commercial as well as business transactions in an easy way [2]. It reduce costs, minimize risk and get faster access to your money by converting paper checks into electronic transactions right at the point of sale.

II. LITERATURE REVIEW

Yaser Esmaeili Salehani et al. [3] has proposed a new dedicated 256-bit hash function:NESHA-256. It has used advantages of parallel structures with the ideas from the designing procedure of block-cipher-based hash functions strengthen our proposed hash function both in security and in efficiency. NESHA-256 is designed not only to have higher security but also to be faster thanSHA-256.

Shay Gueron [4] has shown the comparison of SHA-512 and SHA-256. The reason why SHA-512 is faster than SHA-256 on 64-bit machines is that has 37.5% less rounds per byte (80 rounds operating on 128 byte blocks) compared to SHA-256 .

Masoud Nosrati [5] has proposed a novel techniques of audio steganography. Basic concepts of audio steganography were mentioned and some recent approaches were investigated.

Ritu Pahal [6] has presented a new AES model having bigger block size which is 200 bits rather than conventional 128 bits AES. Also, the block is made by 5 rows and 5 columns unlike the AES's 4 rows and 4 columns.

Deepak Kumar, Research Scholar, Maharishi Dayanand University

Florian Mendel [7] proposed the concept of reducing steps in SHA-256. It has been observed how the attack techniques are used successfully against SHA-1. also, the problems that occur on applying SHA-1 were also investigted. Their methods to resolve them were found.

Kazumaro Aoki [8] has proposed about several techniques to use SHA-1 and MD5 in a more collision resistant manner. The simplest approach which they have discussed in this paper is the message whitening approach. These approaches are both easy to implement, support streaming message digesting, and are amenable to analysis with respect to the known differential attack.

Moni Naor [9] has designed secure cryptographic schemes.

Gabriel Macharia Kamau [10] has presented the comparison of the traditional least significant bit algorithm with the work proposed. The data hiding steganographic method presented in this paper was found to demonstrate increased imperceptibility to statistical steganalysis attacks on the cover image. The hiding capacity can also be increased by varying the number of bits used per color channel. However this method is best suited for the purposes of communication and communication applications as more permanent aspects of steganography like watermarking are not included.

Alan Kaminsky [11] presented the results of a study on the currentprogress of cryptanalysis research on the Advanced EncryptionStandard (AES). The objective was to specifically identify threats and vulnerability trends in secure military,communication applications. Andrey Bogdanov presented a novel technique of block cipher cryptanalysis with bicliques.

Bart Preneel [12] proposed the importance of hash functions for protecting the authenticity of information has been demonstrated. Some theoretical results are also illustrated to support practical constructions, but most of our knowledge on practical schemes is originating from trial and error procedures by several independent researchers and that they are not implemented too quickly.

Sos S. Agaian [13] proposed new method of audiosteganography that allows character data to be encoded into audio in a way that is indiscernible to prying third-parties. The method proposed in this paper provides for a reasonably high-bandwidth and is resistant to common detection and prevention techniques.

III. PROPOSED WORK

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The importance of reducing a chance of the information being detected during the transmission is becoming an issue. Another problem is that people hike the signature of the sender and use it illegally. They send data by using the identification of sender. So it is very necessary to protect signatures from the attackers.

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Steganography. Steganography is a technique of hiding information in digital media [14]. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. We propose the architecture to resolve existing fraud issues.

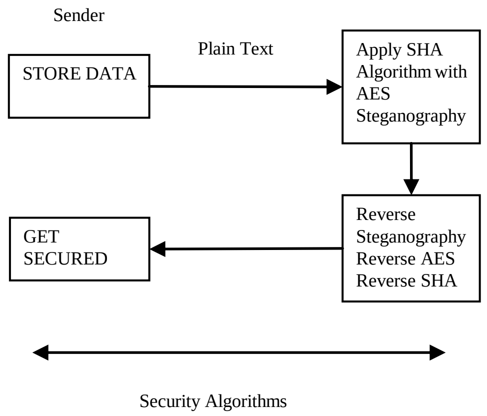

Sender
STORE DATA
Plain Text
Apply SHA Algorithm with AES Steganography
Reverse Steganography Reverse AES Reverse SHA
GET SECURED
Security Algorithms

Figure 2: Architecture of Proposed Work

This architecture given in Figure 2 is used for highly secured e-check by using some security features to enhance the security while transferring cheque from sender to receiver. Now people are using paper cheques just to get security but there are lots of disadvantages/limitations of using paper cheques.

The disadvantage could be the possible fraud by some merchants, also hacking into the electronic records or interception of a transmission is another risk. There is also the danger of human error or equipment failure which can jeopardize the accuracy of transmissions or records. Customers should check their banking records carefully for unfamiliar or unauthorized transactions. So, e-cheques are not much secure until unless some security does not provided to it. So as the solution to the problem we provide “e-cheque with high security“ by using some security concepts explained below:

3.1 SHA 541 (Digital Signature Algorithm): SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS) [15]. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 currently consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits.SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in FIPS PUB 180-4. The SHA-2 family of algorithms are patented in US 6829355. The United States has released the patent under a royalty-free license.

3.2 AES (Advanced Encryption Standard): The Advanced Encryption Standard is a Federal Information Processing

Standards (FIPS) cryptographic algorithm, approved in 2001, that can be used to encrypt and decrypt electronic data [16]. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data blocks of 128 bits.AES is currently used to encrypt government classified information up to the Top Secret level [17].

3.3 Steganography: Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message [18] The goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hiding copyright notice or serial number or even help to prevent unauthorized copying directly [19].

IV. IMPLEMENTATION

In this architecture, sender (bank) will create a cheque & then transfer this cheque to the receiver as a plaintext (original cheque). If any user wants to transferring filled cheque to the intended receiver then its security becomes compulsory. so we can apply security algorithms i.e. DSA (Digital Signature Algorithm):- Electronic Signature can prove the Authenticity of Alice as a sender of the message [20]. DES(Digital Encryption Standard):- DES was designed by IBM and adopted by the U.S. government as the standard encryption method [21].

After applying security algorithms plaintext is converted into cipher text (encrypted message). Then user again apply reverse techniques to get the original message. Then encrypted message again converted into plaintext (original message) in secured manner.

We have implemented this in the .NET Framework which is an integral Windows component for building and running the next generation of software applications and Web services using C#. The backend used is SQL Server 2008.

The snapshots are given from Figure 3 to Figure 8 .

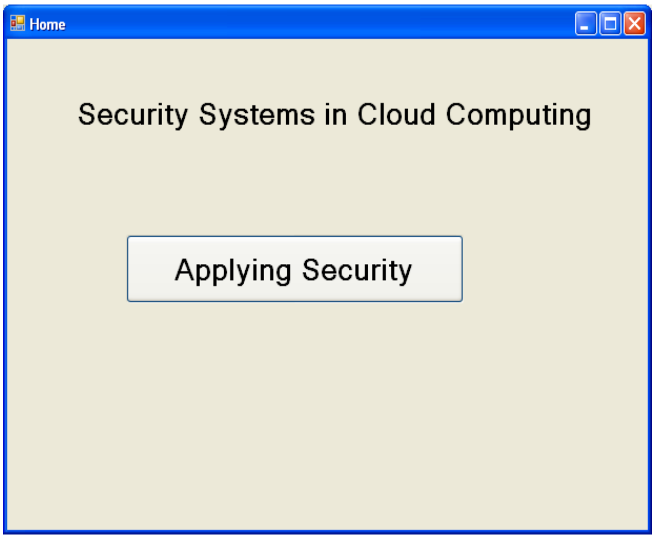


Figure 3 : Welcome Screen

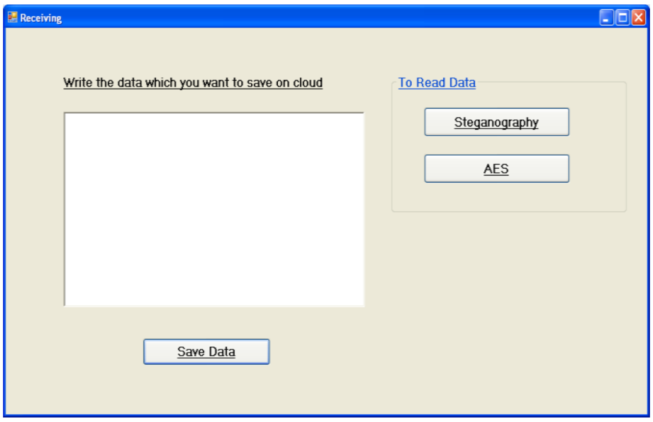
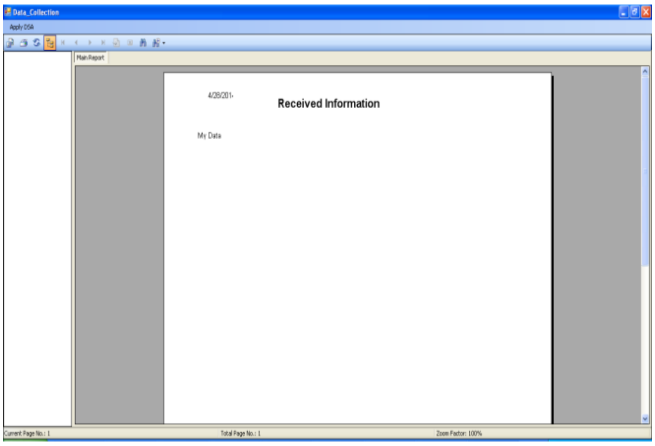


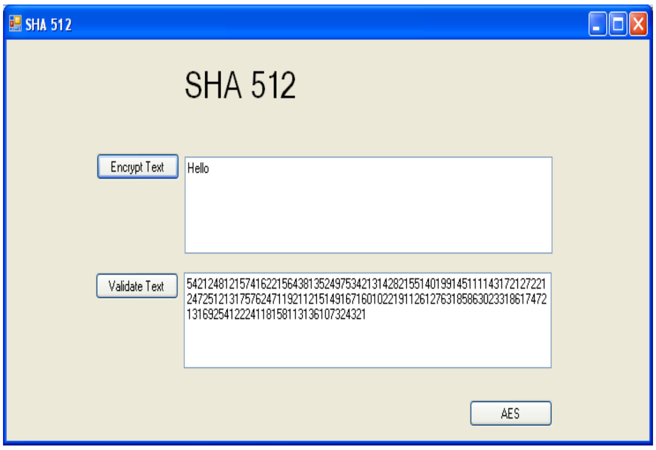
Figure 4: Home Page



4/26/201·

My Data

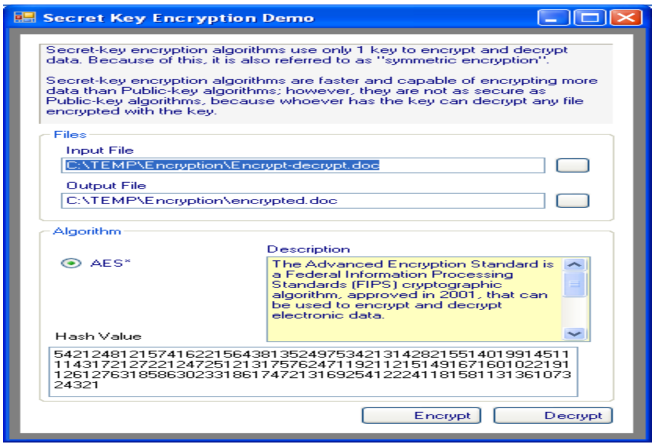
Figure 5: Report of The Data



Hello

```
5421248121574162215643813524975342131428215514019914511114317212722l
2472512131757624711921121514916716010221911261276318586302331861747 2
131692541222411815811313610732432 1
```

Figure 6: SHA-512 (Digital Signature)



Secret-key encryption algorithms use only 1 key to encrypt and decrypt data. Because of this, it is also referred to as "symmetric encryption".

Secret-key encryption algorithms are faster and capable of encrypting more data than Public-key algorithms; however, they are not as secure as Public-key algorithms, because whoever has the key can decrypt any file encrypted with the key.

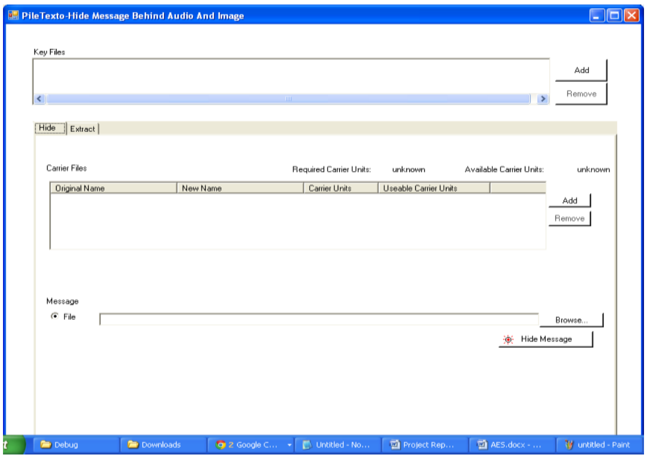
Input File: C:\TEMP\Encryption\Encrypt-decrypt.doc

Output File: C:\TEMP\Encryption\encrypted.doc

The Advanced Encryption Standard is a Federal Information Processing Standards (FIPS) cryptographic algorithm, approved in 2001, that can be used to encrypt and decrypt electronic data.

```
5421248121574162215643813524975342131428215514019914511
1143172127221247251213175762471192112151491671601022191
1261276318586302331861747213169254122241181581131361073
24321
```

Figure 7 : AES (Advanced Encryption Standard)



Required Carrier Units: unknown

Available Carrier Units: unknown

Figure 8: Stegnography

V. CONCLUSIONS

This research work discusses a user friendly Electronic Check System to overcome the limitation of manual check system & to enhance the flexibility of the commercial as well as business transactions in an easy way. It Reduces cost, minimize risk and get faster access to your money by converting paper checks into electronic transactions right at the point of sale. It eliminates the need of issuing cheque-book from the bank. It eliminates cheque portability issue. It provides a more secure means of transaction. It provides a very fast and reliable means of transaction. It lowers the transaction processing time or the clearing cycle. It eliminates the need of internet banking infrastructure (for fund transfer) by the banks. It maintains the confidentiality and integrity of the transaction details. It provides an improved customer service. This kind of e-Cheques management is not being developed and used in any of the Banks so far. This reduces the work load on bank to clear the e-cheques. We use the concept of high security using some security algorithms. These schemes ensure security of the e-cheque (messages) and the signatures can be verified using a digital signature. It is a flexible solution for any cryptographic system and security layers of wireless protocol, such as Hiper LAN/2 and WAP. The proposed design provides high-speed performance and minimized covered area. In future, we can implement our work on the large scale i.e. for large no of users. We can put a help section to show and give any particular help and information about the facilities provided by the software.

REFERENCES

[1] Kumar, A., K.M. Pooja, 2010." Steganography- A Data Hiding Technique, Research paper" , International Journal of Computer Applications (0975 – 8887) Volume 9– No.7.

[2] Sunitha, N. R., B. B. Amberker, and Prashant Koulgi.2007. "Transferable e-cheques using Forward-Secure Multi-signature Scheme." The World Congress on Engineering and Computer Science.

[3] Salehani, Y.E., Hossein, S.A., A.E. Tabatabaei , Abyaneh, R.S., Hassanzadeh ,"NESHA-256, NEw 256-bit Secure Hash Algorithm", Sharif University of Technology, Tehran.

[4] Gueron , S., Johnson , S., Walker , J.," SHA-512/256" Security Research Lab, Intel Labs, Intel Corporation, USA.

[5] Nosrati, M., Karimi , R., Harir, M., 2012. "Audio Steganography: A Survey on Recent Approaches" World Applied Programming, Vol (2), No (3), 202-205.

[6] Pahal, R., Kumar, V., 2013. " Efficient Implementation of AES" SGI Samalkha, Haryana, India Volume 3, Issue 7.

[7] Mendel, Florian, et al. 2009. "Improved cryptanalysis of the reduced Grøstl compression function, ECHO permutation and AES block cipher." Selected Areas in Cryptography. Springer Berlin Heidelberg.

[8] Aoki, K., Sasaki, Y., 2008. " Preimage attacks on one-block MD4, 63-step MD5" . In Selected Areas in Cryptography'08, volume 5381 of Lecture Notes in Computer Science, pages 103–119. Springer.

[9] An Introduction to Cryptography and Digital Signatures Author: Ian Curry March 2001 Version 2.0

[10] Kamau G.M., Kimani, S., Mwangi, W. 2012. "An enhanced Least Significant Bit Steganographic Method for Information Hiding Journal of Information Engineering and Applications, ISSN 2224-5782 (print) ISSN 2225-0506 (online), Vol2, No. 9.

[11] Kaminsky, Alan, Michael Kurdziel, and Stanisław Radziszowski. 2010."An overview of cryptanalysis research for the advanced encryption standard." MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010. IEEE.

[12] Preneel, Bart. 1993. " Analysis and design of cryptographic hash functions." Diss. PhD thesis, Katholieke Universiteit Leuven.

[13] Agaian, S.S., Akopian, D., A. D'Souza1, S. "Two algorithms in digital audio steganography using quantized frequency domainembedding and reversible integer transforms", USA.

[14] Silman, J. 2001. "Steganography and Steganalysis:An Overview", SANS Institute.

[15] National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

[16] A. Biryukov, 2005. "The Boomerang Attack on 5 and 6-Round Reduced AES",LNCS 3373, pp.11-15, Springer.

[17] J. Daemen, V. Rijmen, 1999 ."AES Proposal: Rijndael, Version2", http://www.esat.kuleuven .ac.be/vijmen/rijndael.

[18] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm", Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan

[19] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,www.liacs.nl/home/tmoerl/privtech.pdf

[20] Bellare,M., Miner,S. 1999. A Forward-Secure Digital Signature Scheme. In: Wiener, M. (eds.):Advances in Cryptology-Crypto 99 proceedings,LNCS, Vol.1666, Springer-Verlag.

[21] M. Matsui, 1994."Linear Cryptanalysis Method for DES Cipher",EUROCRYPT, LNCS 765, pp.386-397, Springer.